Magic Quadrant for Security Information and Event Management

8 October 2025 - ID G00822919 - 50 min read

By Andrew Davies, Eric Ahlm, and 2 more

SIEM technology will continue to evolve through multiple features and deployment models to deliver a security system of record with comprehensive threat detection, investigation and response capabilities. This research helps security and risk management leaders evaluate providers in this space.

Market Definition/Description

Security information and event management (SIEM) is a configurable system of record that collects, aggregates and analyzes security event data from on-premises and cloud environments. SIEM processes security event data for the purposes of threat detection, investigation and response. It natively supports data normalization and offers user-configurable detection content and reporting to orchestrate threat mitigation and satisfy compliance requirements. These solutions are delivered via a SaaS platform or client-hosted on-premises or private cloud.

The security information and event management (SIEM) system must assist with:

- Aggregating and normalizing data from various IT and operational technology (OT) environments.
- Designing and executing near real-time monitoring and alerting content.
- Enriching and investigating security events of interest.
- Supporting manual and automated response actions.

- Maintaining and reporting on current and historical event data.

Mandatory Features

- Collection of infrastructure details and security-relevant data from a wide range of assets located on-premises and/or in cloud infrastructure.
- Flexible data retention options for storing essential event data long term and/or making it available for long-term searching.
- Ability for end-users to self-develop, modify and maintain threat detection use cases utilizing correlation-, analytic- and signature-based methods.
- Vendor-provided content for security detection and response (analytics, data normalization, collection correlation, and enrichment and reporting) for both native and non-native solutions.
- Capability to create and customize detection and response content.
- Report generation to support business, compliance and audit needs as required.
- Client-created workflow augmentation capability to support incident response activities and reporting.
- Ability to investigate, evidence and report on discovered security alerts generated by active detection content.

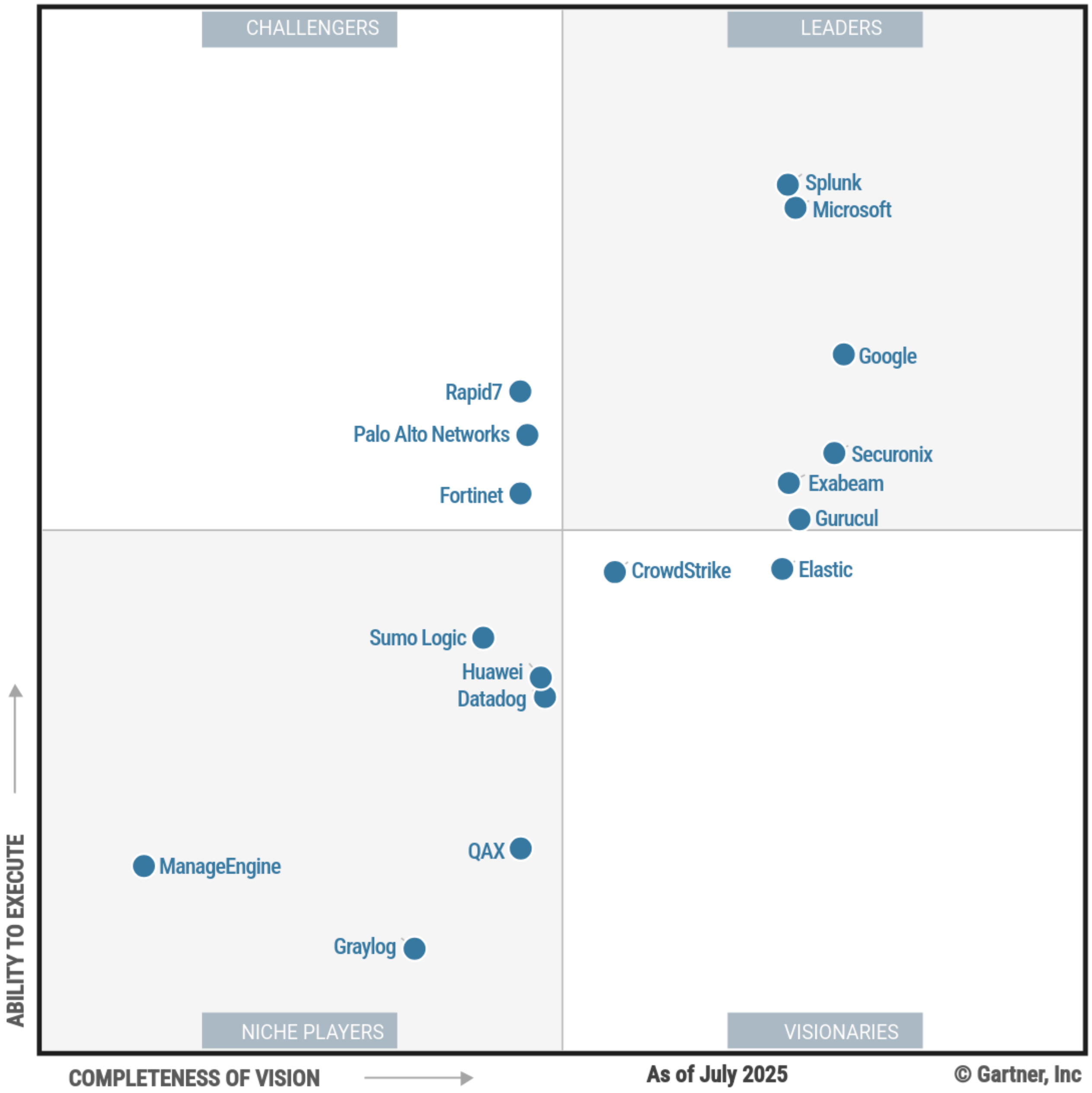
Common Features

- Allow for mixed methods of data collection that includes both streaming event data and static telemetry such as file processing, API retrieved or system configuration data.
- Multiple deployment options to include on-premises, cloud-hosted, cloud-native or SaaS.
- Normalization, enrichment and risk-score data ingestion from third-party systems, such as threat intel sources or configuration management databases (CMDB).
- Provision of case management process and support of incident response actions.
- Workflow augmentation features, such as automation, orchestration of common tasks and use of AI.

- The ability to use various data science techniques to generate detections on a wide range of behaviors, such as user, network, applications or objects, that indicate attack activities.
- Threat intelligence platform (TIP) capabilities to manage intelligence feeds and supply contextual information about threats that may include native threat intelligence.
- A marketplace that allows clients to subscribe to threat content and facilitate integration with third-party technologies.
- Federated search into diverse vendor SIEM environments that allows for analysis and function using a centralizing interface.
- Decentralized search functionality to query events from outside the vendor data repository and pull in additional enriching information where appropriate.
- Extended detection and response (XDR) interoperability that includes the use of endpoint (EDR), network (NDR) or other extended telemetry and response capabilities.
- Third-party data lake platform integrations for storage and search.

Magic Quadrant

Figure 1: Magic Quadrant for Security Information and Event Management



Gartner

Vendor Strengths and Cautions

CrowdStrike

CrowdStrike is a Visionary in this Magic Quadrant. CrowdStrike's product, Falcon Next-Gen SIEM, is offered as a SaaS solution. There is an on-premises and SaaS product, known as Falcon LogScale, which is the log management product within Next-Gen SIEM and is not part of this evaluation. CrowdStrike is well known for its Falcon Complete Next-Gen MDR offering, which also now supports managing the SIEM tool. Its clients are mainly midsize and enterprise-scale. Licensing is based on a gigabytes per day ingest rate with limited free third-party data ingestion for Falcon platform customers.

Strengths

- **Simple, extensible natural language query interface:** Next-Gen SIEM's query interface offers extended features such as threat intelligence enrichment, incident analysis and threat hunting. A query library and autocomplete feature speeds up hunts for new users, and natural language query using Charlotte AI gives analysts a better vision of their environment.

- **Incident management:** Next-Gen SIEM offers in-depth case and incident management functionality. Investigators can collaborate, track workflow status, capture metrics and assign tasks with a broader team working on incidents within the platform.

- **Strength in innovation:** CrowdStrike has focused heavily on SIEM technology, streamlining its roadmaps, allowing it to catch up and deliver future SIEM technologies. Its capabilities for IDR and workflow augmentation with AI showcase its product's strength.

Cautions

- **Lacking data-lake integrations:** Next-Gen SIEM is unable to query and display live data from third-party systems such as data lakes (e.g., Snowflake, Databricks), which require data to be within the Next-Gen environment for analysis.

- **Maturing offering:** Although CrowdStrike has a vast ecosystem of partners and broader platform user base, the limited pool of qualified specialists for CrowdStrike Next-Gen SIEM may hinder an organization's ability to set up customized detection systems.

- **Vendor ecosystem dependency:** Organizations that are not ready to embrace the suite of CrowdStrike offerings may struggle to justify the value of Next-Gen SIEM. That's because its value is greatest when integrated with CrowdStrike's full product suite.

Datadog

Datadog is a Niche Player in this Magic Quadrant. Its product, Datadog Cloud SIEM, is available as a SaaS solution, with some components (e.g., Observability Pipelines) enabled for collection in on-premises deployments. Clients using Datadog's integrated Threat Management suite can expect streamlined playbook creation. Together, small and midsize North American clients make up the majority of Datadog's client base, with a growing presence in larger enterprises. Licensing is available based on millions of events per month, analyzed with flexible storage options. Datadog also offers licensing options for its security orchestration, analytics and reporting (SOAR) tool based on the number of workflows in use per month.

Strengths

- **Converged security and observability:** Datadog offers support for both observability and security monitoring. This is a strength for organizations that want to combine cloud and security signals on a single platform for greater visibility into activity across both domains.
- **Robust query capability:** The product allows organizations to perform advanced queries, including options like creating lookbacks, kicking off investigations from queries or setting up streaming or batch analysis on both security and observability data.
- **Flexible licensing options:** Datadog offers flexible licensing for both observability and security data consumption that allows organizations to better control their costing, even on large volumes of data ingestion.

Cautions

- **User experience:** Organizations may find Datadog's user experience limited for some security outcomes. The product includes features such as dashboards, case management and alert enrichment, but it lacks some investigation features found in other leading SIEMs.
- **Workflow augmentation:** Datadog's ability to augment workflows comes from its SOAR. The development and use of SOAR playbooks is possible. However, they have fewer out-of-the-box playbooks. Datadog still supports strong integration with other SOAR solutions for more complex needs.
- **Security feature velocity:** Datadog's vision for security SIEM is observability-focused. This is common among providers that share security and observability features on a converged platform. Datadog scored lower than average on extended security integrations and case management.

Elastic

Elastic is a Visionary in this Magic Quadrant. Its Elastic Security is focused on providing a unified platform for threat detection, investigation and response across diverse environments. Its operations are mostly focused on North America and Europe, and its clients tend to be large enterprises. Elastic security is available as hosted, serverless and on-premises deployments. Licensing is based on storage-based and compute-based pricing models for Elastic Security. Elastic has continued investing in its Elastic AI, and has delivered integrated onboarding, triage, detection and response workflows using its AI-driven security analytics solution.

Strengths

- **Query language performance:** Clients can build, save and schedule complex queries, and use query performance tools to ensure that they run as anticipated and don't overconsume resources.
- **Threat modeling:** The Attack Discovery feature within Elastic Security aims to streamline security operations by analyzing alerts and presenting them as cohesive attack chains, enabling in-depth correlation analysis, not just detection.
- **Express migration:** Elastic has made strong investments in migration strategies, using its strong API integrations, AI-based Automatic Import, which enables clients to translate between old and new platforms, and automates the development of data integrations.

Cautions

- **UEBA features:** While Elastic Security does provide UEBA functionality, advanced users may find customization, tuning and debugging challenging for advanced detection use cases.
- **Native workflow augmentation:** Elastic, at the time of evaluation, lacks any internal workflow augmentation solutions.
- **Limited language support:** Elastic has a lower-than-average number of languages supported by its platform. Clients with a global presence will need to ensure the languages supported will be sufficient for their global environments.

Exabeam

Exabeam is a Leader in this Magic Quadrant. Exabeam's solution is the Exabeam New-Scale Platform, which is available for SaaS deployments. There is an on-premises product, known as LogRhythm SIEM, which is not part of this evaluation. Exabeam continues to expand its centralized management and monitoring of the data pipeline to support enhanced parsing, event building, enriching and data filtering. It also supports troubleshooting for better service health monitoring, clear error messaging and alerting. The majority of Exabeam customers are in North America and Europe, with a growing presence in Asia/Pacific. Most customers are large enterprises. Licensing is based on the data volumes ingested.

Exabeam and LogRhythm closed their merger on 17 July 2024, during the period the Magic Quadrant and Critical Capabilities research process was being conducted. At the time of publication, New-Scale had met the inclusion criteria, and its LogRhythm product did not meet the functional inclusion criteria requirements.

Strengths

- **Security-centric operations:** The Exabeam user interface prioritizes security analyst needs. Risk scoring and machine learning help in using both UEBA and correlation-rule-based detections, and generative AI Exabeam Copilot helps simplify triage and prioritize investigations for security analysts.
- **Marketplace and content:** Exabeam offers a large amount of content on its marketplace that helps SIEM users achieve results sooner. Notable is its content on insider threat, correlation rules and extensible dashboards to support role-based usage.
- **Use of third-party data:** Exabeam continues to excel at using third-party data for analysis and visualizations, through API and federated searches. SIEM buyers benefit by getting deeper insights without having to ingest from other larger sources of data along with reducing SIEM cost bloat.

Cautions

- **Product competition for resources:** Going from six products to two as a result of Exabeam's merger with LogRhythm temporarily impacted company resources, prioritizing product consolidation over new features. As is common with mergers and acquisitions (M&A), investment allocation among products introduces difficult resource decisions and can impact progress against roadmap goals.
- **Above-average cost:** The Exabeam New-Scale platform's selling price is above average for vendors in this research. Potential customers for whom price is the deciding factor should consider this.
- **Onboarding time:** Exabeam Advanced Analytics (the legacy behavioral detection engine) requires a higher-than-average amount of professional service days to configure.

Although most environments are enterprise level, this is more than other vendors' solutions evaluated as part of this research.

Fortinet

Fortinet is a Challenger in this Magic Quadrant. Its SIEM solution, FortiSIEM, is available as a cloud, on-premises or SaaS solution. FortiSIEM includes Advanced Agents (for Windows-based UEBA). On-premises deployment pricing is based on concurrent users for SOAR, devices' events per second (EPS) and the number of agents for SIEM. FortiSIEM Cloud pricing is based on both compute and storage. Fortinet has matured its TDIR platform vision by investing in FortiCNAAP, FortiDLP and FortiMail Workspace Security. Licensing is based on devices with both perpetual and subscription licenses available. It has a global footprint and customers in all major world regions, but primarily in North America and Europe.

Strengths

- **Third-party data utilization:** FortiSIEM supports querying and displaying live data from third-party systems such as data lakes, Amazon Web Services and ODBC connections, allowing expanded distributed data integration.

- **Built-in configuration management database (CMDB):** Fortinet's centralized CMDB helps with IT infrastructure information discovery of devices, users and applications of organizations.

- **Extended integrations:** Fortinet over the last 12 months has acquired a number of solutions FortiCNAPP (formerly Lacework), FortiDLP (formerly Next DLP) and FortiMail Workspace Security (email security) to support the SIEM threat detection, investigation and response.

Cautions

- **Security bundle effectiveness:** Much of the FortiSIEM value depends on organizations adopting a wide range of Fortinet solutions beyond just FortiSIEM.

- **Workflow augmentation:** FortiSIEM lacks the ability to support automation and orchestration outside of the Fortinet family of products, making the purchase of FortiSOAR a required add-on for most clients for workflow augmentation of non-Fortinet solutions.

- **Unguided source integrations:** FortiSIEM supports the ability to create custom parsers for unique log sources using the XML specification. However, unlike other vendors, it does not leverage any form of automated support for this process, requiring a more manual effort to extend the platform.

Google

Google is a Leader in this Magic Quadrant. Its SIEM product, SecOps, is available as a SaaS solution and has been Google's foundational product to help secure enterprise customers, with a focus on large-scale query and analytics capabilities. Google's product enhancements for core SIEM functions and AI flexibility have opened up SecOps as a strong SIEM competitor. Per-user licensing and licensing based on a gigabytes per day ingest rate (for high user or employee populations) are available. Google has a global footprint and customers in all major world regions, but primarily in North America and Europe. Google is continuing to invest in its Gemini AI for content generation, search and investigation, and threat intelligence analysis and summarization.

Strengths

- **Robust search and query:** Google's SecOps platform excels at advanced and complex queries. Its unified data model and query language YARA-L is highly capable in extracting value from the analysis of security signals within detection and investigation workflows.

- **Large enterprise and MSSP ready:** Google's federated and multitenant capabilities make its solution highly attractive to global organizations requiring multiple SIEMs, particularly for the use of a common search query language and ability to push out detection rules. This allows for centralized use case management and distribution.

- **Powerful AI and workflow augmentation:** Use of AI is a core competency for Google and its SecOps platform offers strong AI functionality throughout many of the common activities and functions associated with SIEM operations. Its well-integrated automation capabilities add to this overall strength.

Cautions

- **Cloud-only solution:** Google's SecOps platform is fully cloud-hosted. This may be a detriment to clients who still require some sort of on-premises solution.

- **Complex user interface:** Google takes a programmatic approach to many common functions such as building queries, enrichment and investigations leveraging its YARA-L language. This command-line-type approach is highly deterministic, but it requires an advanced skill set to implement and operate.

- **UEBA features:** Although Google offers advanced analytic functionality, its UEBA still lacks common built-in use cases found in other leading solutions. While it's seen some improvement over the year, it's not as advanced as its peers.

Graylog

Graylog is a Niche Player in this Magic Quadrant. Its SIEM product, Graylog Security, is available as a SaaS or self-hosted solution, with most clients opting for the latter, either as part of an on-premises setup or their own private cloud environment. Users of the tooling can expect easy-to-use dashboards with customization and filters that can be applied to a selection of available widgets. Recently, the platform has been upgraded to include risk-based reporting and UEBA functionality driven by machine learning. Most Graylog clients are primarily based in North America and Europe and are midsize and enterprise-scale clients, making up almost 90% of its total client base. Licensing is available as a gigabytes per day ingest rate.

Strengths

- **Easily customizable query:** Graylog offers an easy-to-use functionality for creating search, active monitoring or correlation rules that helps organizations quickly get use from its security signals.

- **Risk-based alerting:** Graylog's introduction of risk-based alerting and reporting improves organizations' ability to triage alerts and prioritize anomaly-based detections, contributing to faster detection and response times.

- **Simplified operations:** Graylog's wizards and intuitive UX on its SIEM platform will appeal to smaller or less-mature organizations seeking simplified operations.

Cautions

- **Emerging add-on capabilities:** Advanced features such as automation, use of AI or UEBA are still emerging on the Graylog platform. Although Graylog does provide some capability in each of these areas, some organizations might find the functionality limiting.

- **Incident management:** While Graylog has case management capabilities and attack mappings using the MITRE ATT&CK framework to aid incident response, more mature organizations may need to add advanced case management and SOAR playbook capabilities.

- **Enterprise extensibility:** Graylog's limited out-of-the-box third-party integrations may make the use of its solution in highly mature organizations more challenging.

Gurucul

Gurucul is a Leader in this Magic Quadrant. Gurucul Next-Gen SIEM is available as SaaS, cloud or self-hosted. It offers UEBA, identity analytics/ITDR, data optimizer, SME AI, fraud analytics, network analysis and SOAR. Its extensive use of analytics for building risk-based behavioral detections should appeal to enterprise clients requiring complex and identity-based detections. Gurucul's customer base is composed primarily of large enterprises based in North America and Europe. Gurucul offers flexible pricing options, including all-inclusive per-asset/user pricing, ELAs, module-based, data volume/EPS-based pricing and platform-based pricing.

Strengths

- **Market strength:** Gurucul has expanded its global marketing program in the last year, which can be seen by its consistent year-over-year growth and higher-than-average customer renewals.

- **Pace innovation:** Gurucul's singular focus on SIEM technology has allowed it to streamline its roadmaps and continue to exceed the market in innovation. They have shown a year-over-year ability to deliver on roadmap items consistently and the agility to pivot with market changes.

- **Enhanced data management:** Gurucul data optimizer is its native data pipeline management product. It offers advanced data management and filtering/routing options, allowing clients more flexibility in data streaming to the SIEM to help with costs and data bloat. Its data management capabilities extend to helping manage multicloud environments.

Cautions

- **Built for advanced users:** Gurucul's Next-Gen SIEM includes a large library of content out of the box to get value quickly, but it is more suited to larger and mature security buyers with complex use cases. Smaller or less mature security operations centers (SOCs) may not be able to get the most out of all the features.

- **Market price:** Gurucul is priced higher than its immediate competitors in the space, and companies may have to judge the actual value of the advanced features available versus necessary use cases.
- **Workflow augmentation:** Gurucul offers workflow functionality. However, its solution lacks many of the advanced features found in other leading market solutions.

Huawei

Huawei is a Niche Player in this Magic Quadrant. Its SIEM solutions, SecMaster and HiSec Insight, are available as Huawei public cloud for SaaS, customer private clouds and on-premises. It includes Huawei Cloud SecMaster, with additional modules and companion technologies such as EDR, web application firewalls (WAFs) and host security service (HSS). Deployment options include pricing for on-premises deployments, which are based on data velocity (EPS) and volume (gigabytes per day), with additional charges for log retention and add-on modules. SaaS deployments are based on a gigabytes per day ingest rate. Its SIEM customers are largely concentrated in Asia, although a smaller number of clients are based in the Middle East, Africa and Latin America.

Strengths

- **Enhanced enterprise support:** Huawei's SIEM offers enterprise features such as automation, customizable dashboards and use of native threat intelligence for enrichment.
- **AI-ready workflows:** Huawei has been working to increase the use of AI to augment workflows throughout the SIEM. Use cases such as suggestive automation, AI-powered alert enrichment and attack path analysis are part of its current capabilities.
- **Evolving product strategy:** Huawei continues to show innovation in its product strategy. It has added or enhanced many must-have enterprise capabilities, evolving its overall solution.

Cautions

- **Limiting query capabilities:** Huawei's lack of federated search and nonembedded AI query capabilities, specifically in the interface, still trail the competitive field in terms of features or capabilities.

- **Geographic strategy:** Huawei's geographic strategy focuses primarily on Asia/Pacific, the Middle East, Latin America and Africa. Organizations outside of those regions specifically might find limited technical support, lack of region-specific SaaS offerings and lack of language support as barriers.

- **Deployment:** Professional services are necessary for Huawei's more complicated deployments. This may incur substantial additional costs for companies that don't have expertise in SIEM deployments.

ManageEngine

ManageEngine, a division of Zoho Corporation, is a Niche Player in this Magic Quadrant. Its SIEM solution, Log360, is cloud-based and deployed from its data center. UEBA, SOAR and data loss prevention (DLP) are included as add-ons in the SaaS license. In addition, ManageEngine offers security products such as Firewall Analyzer, Vulnerability Manager Plus and FileAnalysis. ManageEngine continues to invest in its Vigil IQ engine to enhance advanced threat detection use-case support, expanded vendor integrations and an attack surface analyzer. Licensing is based on the amount of gigabytes per day stored in the cloud with customizable retention periods. Its customers are primarily large and midsize enterprises that are located in North America, Europe and Asia/Pacific.

Strengths

- **Workflow augmentation:** The Qntrl Circuit (formerly Zoho Circuit), Zoho's automation platform, enhances Log360 by introducing automation and orchestration capabilities, offering a unified interface with other Zoho solutions.

- **Unified ManageEngine experience:** To reduce user complexity, ManageEngine's Log360 platform provides a unified experience by integrating threat detection and incident response capabilities with its other tools, such as EventLog Analyzer, ADAudit Plus, ADManager Plus, M365 Manager Plus, Exchange Reporter Plus and Cloud Security Plus.

- **Dark web integration:** Through its integration with Constella Intelligence, ManageEngine Log360 provides proactive detection and response for dark web threats. This allows organizations to promptly identify compromised credentials and take immediate action to revoke them, strengthening their security defenses.

Cautions

- **Simplicity focus:** ManageEngine’s target market and current customer base are largely composed of ease-of-use SIEM users. This means the platform will be better suited to those users with lower customization-driven requirements and may not be suitable for larger, more mature users.

- **Product development:** ManageEngine’s Log360 currently lacks robust augmentation by AI. Its feature sets lag behind market leaders for advanced applications of AI into common workflows.

- **Operational technology (OT) support:** Log360 currently lacks any native monitoring of OT environments and does not have any third-party technology integrations that other SIEM vendors have created.

Microsoft

Microsoft is a Leader in this Magic Quadrant. Its SIEM solution is Microsoft Sentinel, which is delivered only as a SaaS offering via Microsoft Azure cloud services. Microsoft Security Copilot enhanced AI has been integrated with Microsoft Sentinel for assistance with incident response as well as integrations with other tools. Microsoft Sentinel’s customer base spans North America, Europe, the Middle East, Africa, Asia/Pacific and Latin America. Customers also range in size from small and midsize businesses to large enterprises. Pricing is based on the volume of data analyzed in Microsoft Sentinel and is variable based on the level of subscriptions in Microsoft 365 E5, A5, F5 and G that include daily credits. Fees are also levied for data stored in Azure Monitor Log Analytics workspace by retention period and volume. Committed payment tiers and pay-as-you-go models are also available.

Strengths

- **Breadth of integrations:** Integrations into Microsoft Sentinel continue to stand out. Microsoft has expanded its third-party support and continues its native integration strategy with other products such as Microsoft Defender XDR, Microsoft 365 Lighthouse and Microsoft Security Copilot. This can simplify security operations for clients embracing the suite of Microsoft products.

- **Customizable detection analytics:** The Sentinel threat intelligence dashboard provides a fully customizable canvas for reporting on the health and performance of threat intelligence (TI). Microsoft Sentinel customers can build and customize machine learning (ML)-based threat detection as well as leverage out-of-the-box (OOTB) templates.

- **Enhanced AI and MITRE ATT&CK coverage:** Sentinel offers strong MITRE ATT&CK coverage built around the Microsoft security toolset. Microsoft's AI capabilities also allow for more data enrichment and recommendations for correlation.

Cautions

- **Pricing:** Ingestion costs for non-Microsoft data, especially from external sources, can be higher than competitors', posing challenges for cost control and scalability. Geolocation and third-party data ingestion into Microsoft Azure may also cause some variability in cost.

- **Architectural inflexibility:** Sentinel is available only as a SaaS product hosted in Microsoft Azure. Cloud self-hosted and on-premises options are unavailable.

- **Azure skill set:** Detection and workflow engineering within the Sentinel platform will still require extensive Azure knowledge for building integrations with non-native Azure ecosystem telemetry sources.

Palo Alto Networks

Palo Alto Networks is a Challenger in this Magic Quadrant. Palo Alto Networks' (PANW's) SIEM product, Cortex XSIAM, is offered exclusively as a SaaS solution. It has three tiers — XSIAM NG SIEM, XSIAM Enterprise and XSIAM Premium — with each tier priced per knowledge worker. Cortex XSIAM comes with comprehensive and intuitive playbook creation and testing, offering clients varied options for automation in incident response, with an extensive marketplace that helps map playbooks to certain objectives. PANW has integrated XDR and attack surface management (ASM) as well. PANW's clients are mostly large enterprise-sized organizations that can fully leverage the full extent of PANW's tech stack. PANW's acquisition of IBM QRadar on Cloud (QRoC) has helped expand its customer base into the SIEM market. Its SIEM customers are primarily located in North America, with some in Europe, the Middle East, Africa and Asia/Pacific.

Strengths

- **Automation capabilities:** XSIAM's built-in automation, XSOAR, offers an array of functionality to assist SIEM operations, ready-to-use content and natural integration into everyday workflows and activities.

- **Incident management and workflow:** XSIAM provides comprehensive case and incident management functionality. Investigators can set case priorities with AI-assigned risk

- scores, track workflow status, capture metrics, assign tasks and collaborate with a broader team working on incidents within the platform, leveraging its war room feature.
- **MITRE framework integration:** XSIAM has strong integration with the MITRE ATT&CK framework and complex field mapping is available OOTB for security analysts.

Cautions

- **Data mapping:** XSIAM log collection leverages manually updated parsing, making adding custom log sources more complicated than other vendors.
- **Emerging enterprise capabilities:** XSIAM lacks refinement in some OOTB core functionality such as UEBA and dashboards. PANW's OOTB content for UEBA offers basic use-case support, and custom dashboard creation functionality is still emerging.
- **Cost justification:** Although PANW supports third-party devices, XSIAM's cost justification is somewhat dependent on leveraging existing PANW products.

QAX

QAX is a Niche Player in this year's Magic Quadrant. Its NGSOC SIEM solution is part of its SOC solution and it is available in SaaS, cloud or on-premises, with over 80% of clients opting for the on-premises version. QAX's SIEM licensing is based on events per second. Most of its clients are midsize organizations based in Asia/Pacific and Africa, with a few customers in the Middle East, Europe and the Americas. QAX invested in a cross-platform threat correlation engine that uses an LLM to infer attack paths and AI-optimized detection logic to improve detection ability and reduce false positives.

Strengths

- **Enhanced enterprise features:** QAX has expanded its enterprise capabilities with add-ons like UEBA, AI-driven security operations and low-code workflow automation.
- **OOTB dashboards:** QAX offers enterprises a higher-than-average number of predefined dashboards for role-based workflows and reporting options.
- **Direct services:** QAX extends value to midsize enterprises by offering MDR services directly from QAX, providing a single vendor experience for both product and ongoing management services.

Cautions

- **Out-of-the-box detection:** The number of out-of-the-box correlations and analytics available is lower than the average offered by vendors in this Magic Quadrant.

- **Community app store:** QAX lacks an app store where its customers can share workflows, custom detections and parsers. This makes it harder to expand the platform and learn from others.

- **APAC-centric:** QAX predominantly serves customers in one region: Asia/Pacific. From a sales and support perspective, a lack of understanding of local market requirements and restrictions outside of Asia/Pacific can lead to a limited experience for customers with a global footprint.

Rapid7

Rapid7 is a Challenger in this Magic Quadrant. Its SIEM solution, InsightIDR, runs on the SaaS Command platform. Licensing is based on the number of assets monitored with unlimited ingestion. Customers of the InsightIDR SIEM range from small to large organizations. They are concentrated most heavily in the U.S., followed by Europe and Asia/Pacific. Rapid7 offers a premium package called Threat Complete that integrates InsightIDR, attack surface management, and digital forensics and incident response (DFIR) capabilities into investigative workflows in a single package.

Strengths

- **Security-role user interface:** Rapid7's customization capabilities have expanded within the SIEM, allowing SOC engineers and analysts to better adjust rules and reports to meet specific role-based needs.

- **Small and midsize business support:** Rapid7 has a model that supports SMB security needs to get SIEM programs working because its managed detection response service ensures that clients are well-supported and monitored 24/7.

- **Wide range of integrated capabilities:** Rapid7's core SIEM offers many security capabilities, including InsightVM, which provides vulnerability management. It also offers InsightIDR, which has EDR, UEBA, and network detection and response (NDR) capabilities that are highly integrated for a single experience for SOC operators.

Cautions

- **Extensibility:** While Rapid7's product is an independent SIEM, clients will get the most out of InsightIDR when it is used in conjunction with the broader Rapid7 suite of products.
- **Advanced capabilities:** InsightIDR lacks more expanded capabilities, such as advanced analytics (e.g., supervised ML and custom deep-learning analytics) and limited AI support for guidance.
- **OOTB compliance reports:** Rapid7 does not have the breadth of compliance reports and dashboards OOTB when compared to other vendors in this research.

Securonix

Securonix is a Leader in this Magic Quadrant. Its SIEM solution, Unified Defense SIEM, is available as a SaaS and on-premises solution. It includes an embedded Snowflake data lake, UEBA and basic SOAR. Add-ons include advanced SOAR capabilities, Autonomous Threat Sweeper and Investigate, and GenAI. Licensing is via volume (gigabytes per day). Most Securonix customers are in North America, followed by Europe, the Middle East, Africa, Asia/Pacific and Latin America. Securonix's customer base is primarily large enterprises and midsize organizations. Securonix is investing in its Data Pipeline Manager for more cost-effective data ingestion. It is also investing in GenAI agents to improve SOC efficiency with investigation, policy, response and insider agents.

Strengths

- **Third-party data lake access:** Securonix allows organizations to bring their own data lake or other storage solutions to build an SIEM. This gives organizations the flexibility to choose the best independent storage options for different uses such as real-time analytics, long-term storage or threat hunting.
- **UEBA capabilities:** Securonix handles advanced UEBA use cases well. Its solution has extensive out-of-the-box profiles, offers psycho-analytics for unique case development, role-based workflows for insider threat teams and extensive testing and tuning capabilities.
- **Development team size:** Securonix has a larger-than-average team for developing and supporting its roadmap for the upcoming year, ensuring consistent delivery of new features and fixes.

Cautions

- **Emerging workflow augmentation:** Securonix offers Workflow functionality. However, its solution lacks many of the advanced features and integrations found in other leading market solutions.

- **Advanced search and query:** Securonix reliance on risk scoring and real-time analytics can reduce its ability to create advanced manual queries as compared to other competitors in the market.

- **Market execution:** Although a long-standing leader in the SIEM market, Securonix's client adoption growth rate is lower than that of other market leaders. Its product messaging and positioning exist as opportunities.

Splunk

Splunk, a Cisco company, is a Leader in this Magic Quadrant; Cisco completed the acquisition of Splunk in March 2024. Its SIEM application, Splunk Enterprise Security, is an add-on to the Splunk Enterprise solution and can be delivered either on-premises or via SaaS. Splunk offers pricing based on daily ingest or cloud workloads, known as Splunk Virtual Compute, for any deployment model. Splunk has introduced new features, including an AI assistant, to its integrations with Enterprise Security. The majority of Splunk's clients are larger North America-based enterprise organizations.

Strengths

- **Customized for enterprise usage:** Splunk offers a wide range of customization and integration options that help complex organizations build workflows, role-specific dashboards and integrations that support large enterprise needs.

- **Extensive marketplace:** Modern SIEMs depend on continuously updated content and apps to deliver required security outcomes. Splunk's extensive content library and community of developers produce a high number of resources to ensure optimum SIEM performance.

- **Extended integrations:** Splunk continues to expand integrations in the security ecosystem as well as with Cisco products that enhance its product value. For example, through Cisco Talos, Cisco's threat intelligence solution, Splunk users benefit from rich native threat intelligence.

Cautions

- **Limited AI workflow augmentation:** Splunk's integration of AI into a wide range of workflows still lags behind other leading SIEM solutions.

- **Complexity and expertise:** Splunk's customizable platform comes at the price of adding complexity. Less mature organizations may find that the wide range of features causes longer setup times and ongoing operational overhead.

- **Focus on core product improvements:** Splunk slightly trailed other Leaders around its future product roadmap. Splunk continues to focus on improvements and integrations core to its product strategy of a unified TDIR platform, while other competitive solutions execute its vision to evolve its solutions at a faster pace.

Sumo Logic

Sumo Logic is a Niche Player in this Magic Quadrant. Its SIEM product, Sumo Logic Cloud SIEM, is delivered exclusively as a SaaS solution within its unified log analytics platform. In 2024, Sumo Logic introduced Flex Pricing, offering free, unlimited data ingest and aligning costs with data storage and analytics usage, thereby removing traditional cost barriers associated with data volume. This model supports unlimited users and data sources without additional charges. The customer base spans small to large enterprises, predominantly in North America, with a growing presence in Europe, Latin America, and Asia/Pacific. Sumo Logic has accelerated innovation, introducing AI-driven features like the Sumo Logic Copilot assistant for natural language log analysis, AI-driven alerting and the MITRE ATT&CK Threat Coverage Explorer for enhanced threat detection.

Strengths

- **Simplified licensing:** Sumo Logic designed its product to handle large volumes of observability data efficiently and cost-effectively. This beneficially enables security teams to ensure the best use of data, lowering the overall costs often associated with high data volumes on an SIEM.

- **Supports both security and observability:** Sumo Logic's platform is well-suited for organizations that need to ingest and analyze both observability and security data, making it easy to compare signals across both domains. This capability supports use cases involving both security and observability.

- **Detailed MITRE mapping:** Sumo Logic's implementation of the MITRE ATT&CK framework to map alert signals to various tactics and stages of attack helps organizations more accurately and quickly identify and resolve security issues.

Cautions

- **Limited alert enrichment capabilities:** Sumo Logic’s alert enrichment capabilities and use of TI lag behind other security-centric competitors in the market.
- **Emerging workflow augmentation:** Sumo Logic offers limited workflow augmentation. Its automation capabilities lack in-depth integration into workflows and fall short on advanced development and content support.
- **Security feature velocity:** Sumo Logic’s product strategy to service both observability and security teams can leave security teams short on some requirements, such as OOTB content for UEBA.

Vendors Added and Dropped

We review and adjust our inclusion criteria for Magic Quadrants as markets change. As a result of these adjustments, the mix of vendors in any Magic Quadrant may change over time. A vendor's appearance in a Magic Quadrant one year and not the next does not necessarily indicate that we have changed our opinion of that vendor. It may be a reflection of a change in the market and, therefore, changed evaluation criteria, or of a change of focus by that vendor.

Added

- Palo Alto Networks
- CrowdStrike
- Graylog
- Datadog

Dropped

- Devo Technology did not meet the commercial requirements for inclusion in the 2025 Magic Quadrant for SIEM.

- LogRhythm was acquired by Exabeam, which subsequently EOLed LogRhythm Axon. As a result, LogRhythm did not meet the functional requirements for inclusion in the 2025 Magic Quadrant for SIEM.
- IBM did not meet the functional requirements for inclusion in the 2025 Magic Quadrant for SIEM.
- Logz.io did not meet the functional and commercial requirements for inclusion in the 2025 Magic Quadrant for SIEM.
- Logpoint did not meet the functional requirements for inclusion in the 2025 Magic Quadrant for SIEM.
- NetWitness did not meet the functional and commercial requirements for inclusion in the 2025 Magic Quadrant for SIEM.
- OpenText did not meet the functional and commercial requirements for inclusion in the 2025 Magic Quadrant for SIEM.
- Odyssey did not meet the commercial requirements for inclusion in the 2025 Magic Quadrant for SIEM.
- Venustech did not meet the commercial requirements for inclusion in the 2025 Magic Quadrant for SIEM.

Inclusion and Exclusion Criteria

To qualify for inclusion, a vendor needed to fulfill the following criteria:

- A product that provides SIM and SEM capability consumable by end-user customers as cloud-native software and/or SaaS, excluding those that are available only as part of a managed security services relationship (see Note 1). SIM and SEM must-have capabilities are:
  - Collect infrastructure details and security-relevant data from a wide range of assets located on-premises and/or in cloud infrastructure.
  - Ability for end users to self-develop, modify and maintain threat detection use cases utilizing correlation, analytic and signature-based methods.

    - Correlate and apply both SIEM vendor- and client-created analytics to collect, normalize and contextualize event data from disparate sources, using multiple mechanisms (log stream, API, file processing) for the purposes of threat detection, use-case implementation and incident investigation.
    - Provide case management and support incident response activities (see Note 2).
    - Generate reports to support business, compliance and audit needs.
    - Store essential security event data over the long term and make it available for investigation.
- At least 50 vendor-provided collectors for data capture and streaming from heterogeneous third-party data sources via API in addition to data streaming or log collection. This must include formally recognized partnerships with at least 10 major technology vendors.
- A product that supports behavioral analysis and/or correlation of data from sources other than directly from the vendor's product ecosystem, this should include market-leading network technologies, endpoints/servers, cloud (IaaS or SaaS) and business applications.
- Features, functionality and at least two of the following additional capabilities that were generally available, vendor-owned (wholly acquired or organically built) and included in the SIEM as of 31 December 2024:
    - Federated search into distributed environments, able to search across SIEM data repositories (e.g., geographic regions or cloud providers' regions).
    - Search functionality to query events outside the SIEM data repository and to pull in additional enriching information where appropriate.
    - Third-party data lake platform integration and storage.
    - Availability of long-term data storage and reporting (with "hot" recall capability of 365 days).
- Add-on solutions including at least two of the following additional capabilities that were generally available, vendor-owned (wholly acquired or organically built) and included in the SIEM product or sold as separate add-ons as of 31 December 2024:

    - Workflow augmentation, supporting features such as automation and orchestration of common tasks.
    - Threat intelligence platform (TIP).
    - Advanced analytic capabilities using user entity behavior analytics, data sciences (e.g., supervised and unsupervised machine learning, deep learning/recurrent neural networks).
- Cloud-native/SaaS license and maintenance (excluding managed services) revenue exceeding $85 million for the 12 months prior to 31 December 2024, or have 500 distinct production customers with direct contracts on cloud-native or SaaS platforms as of the end of that same period (see Note 3).
- In the 12 months prior to 31 December 2024, to have received 25% of SIEM cloud-native/SaaS revenue from buyers with headquarters outside the geographic region of the vendor’s headquarters location, or have at least 25% of production customers, each with headquarters outside the geographic region of the vendor’s headquarters location (see Note 4).
- Evidence of online marketing campaigns, events or promotions from third-party media sources targeting countries in at least two geographic regions, distributed prior to 31 December 2024.
- Cloud-native/SaaS SIEM platform hosted in more than three major geographic regions.
- New customer acquisition or competitive replacement above 5%.

Honorable Mentions

- **Anvilogic** did not meet the commercial requirements for inclusion in the 2025 Magic Quadrant for SIEM. However, it is considered an option for buyers who are focused on having an analytics layer on top of their data lake.
- **Panther** did not meet the commercial requirements for inclusion in the 2025 Magic Quadrant for SIEM. Panther offers a SIEM powered by data lake technologies such as Snowflake, which gives users requiring higher data ingestion more options for data management. Panther also offers detection as code capabilities that aid in creating more robust detection content.

- **Hunters** did not meet commercial requirements for inclusion in the 2025 Magic Quadrant for SIEM. Hunters provides machine-powered ingestion, detection, triage and investigation based on a security data lake architecture. It offers unlimited ingestion per entity, which is best for buyers looking to have cost predictability.
- **SentinelOne** did not meet the inclusion criteria for consideration in the 2025 Magic Quadrant for SIEM. Its AI SIEM offers complexity reduction of SIEM operations both by leveraging integrations with its ecosystem of other security solutions and by the application of AI to aid in analysis and general workflow augmentation.

Evaluation Criteria

Ability to Execute

Product or service: This criterion evaluates a vendor's ability to provide product functions in core SIEM areas, such as the ability to create, modify and maintain threat detection use cases. It also assesses the vendor's capacity to provide case management, support incident response activities, and generate reports to support business, compliance and audit needs.

Overall viability: This criterion includes an assessment of a vendor's customer traction, the financial and practical success of its SaaS SIEM business and indicators that it will continue to invest in SIEM technology.

Sales execution/pricing: This criterion evaluates a vendor's success in the SIEM market and its capabilities in presales activities. Considerations include the size of its SIEM revenue and installed base for its cloud-native/SaaS SIEM revenue and installed base, flexibility of pricing models, its presales support, and the distribution and inclusion of its sales channel. The level of interest and reviewed experiences from Gartner clients are also considered.

Market responsiveness/record: This criterion evaluates the delivered features and alignment to client demand for adjacent SIEM capabilities and modern deployment methods. It also assesses the track record of delivering new and differentiated functions in line with the changing needs of the market. Considerations include support for multicloud monitoring, cloud-native and SaaS business focus, and industry-specific support within areas such as OT.

Marketing execution: This criterion evaluates a vendor's SIEM market messaging in light of Gartner's understanding of customer needs. Promotion of the brand, increasing awareness of products and influence on the SIEM market are evaluated.

Customer experience: This criterion evaluates product function and service experience in production environments. Included are operations, administration and vendor support capabilities. This criterion assesses areas such as available support and training and customization of user interfaces.

Operations: This criterion evaluates a vendor’s service, support and sales capabilities. It includes an assessment of these capabilities across multiple geographies.

Ability to Execute Evaluation Criteria

Evaluation Criteria	*Weighting*
Product or Service	High
Overall Viability	Medium
Sales Execution/Pricing	High
Market Responsiveness/Record	High
Marketing Execution	Medium
Customer Experience	Medium
Operations	Medium

Source: Gartner (October 2025)

Completeness of Vision

Market understanding: This criterion evaluates a vendor’s ability to understand buyers’ emerging needs and how to communicate solutions effectively. SIEM vendors that show the highest degree of market understanding can identify how technology and changes in ways of working will translate into modern security operations requirements, while also meeting the business risk and ROI needs of organizations.

Marketing strategy: This criterion evaluates a vendor's ability to communicate the value and competitive differentiation of its SIEM offering.

Sales strategy: This criterion evaluates a vendor's use of direct and indirect sales, marketing, service and communications affiliates to extend the scope and depth of its market reach.

Offering (product) strategy: This criterion evaluates a vendor's approach to product development and delivery, with an emphasis on how well functionalities and features correspond to current requirements. Development plans during the next 12 to 18 months are also evaluated. The SIEM market is mature — there is little differentiation between most vendors in areas such as support for common network devices, security devices, OSs and consolidated administration capabilities. We assign higher weightings to coverage of emerging event sources, such as IaaS and SaaS, and environmental context.

Despite vendors' focus on expanding their capabilities, we continue to value simplicity of deployment and ongoing support. Users, especially those with limited IT and security resources, still value this attribute over breadth of coverage beyond basic use cases. SIEM products are complex and tend to become more so as vendors extend their capabilities. Vendors able to provide effective products that users can successfully use as a service, or deploy, configure and manage with limited resources, will be the most successful.

Vertical/industry strategy: This criterion evaluates a vendor's strategy to support SIEM requirements specific to industries, like operational technology environments.

Innovation: This criterion evaluates a vendor's development and delivery of SIEM technology that is differentiated from that of its competitors in a way that uniquely meets customers' most important requirements. Product capabilities and customer use in areas such as application layer monitoring, identity-oriented monitoring and incident investigation are evaluated. This is in addition to other product-specific capabilities that are needed and deployed by customers. Heavy weightings are assigned to capabilities needed for advanced threat detection and incident response: user, data and application monitoring; ad hoc queries; visualization; orchestration and incorporation of context to investigate incidents; and workflow/case management features.

Geographic strategy: This criterion takes account of the fact that, although the North American and EMEA markets produce the most SIEM revenue, Latin America and Asia/Pacific are growth markets for SIEM. Additionally, their growth is driven primarily by demand for threat management (and secondarily by compliance requirements). Our overall evaluation of vendors in this Magic Quadrant includes an evaluation of their sales and support strategies for those regions as well as product features to support local and regional compliance requirements for data residency and privacy.

Completeness of Vision Evaluation Criteria

Evaluation Criteria	*Weighting*
Market Understanding	High
Marketing Strategy	Medium
Sales Strategy	Low
Offering (Product) Strategy	High
Business Model	NotRated
Vertical/Industry Strategy	Medium
Innovation	High
Geographic Strategy	Medium

Source: Gartner (October 2025)

Quadrant Descriptions

Leaders

Leaders consistently show evidence of superior vision and execution for emerging and anticipated requirements. Leaders provide products that are a strong functional match for the market's requirements. These vendors have been the most successful at building an installed base and revenue stream in the SIEM market. In addition to providing technology that is a good match for current customer requirements, the evolving state of the SIEM market presents new visions of what a SIEM can be. This has challenged the status quo of what it takes to be a leader. They typically have a relatively high market share and/or strong revenue growth and receive positive customer feedback about their SIEM capabilities and related service and support.

Challengers

Challengers have multiple product and/or service lines, at least a modestly sized SIEM customer base, and products that meet a subset of the market's general requirements. They also have strong market visibility, resulting in better Ability to Execute compared to Niche Players. However, Challengers are often late in addressing emerging needs, lack depth in product integration, and may have accumulated technical debt, which affects usability. They may also lack alignment with the market's direction, impacting their Completeness of Vision compared to Leaders. Challengers are practical choices, especially for customers with established strategic relationships.

Visionaries

Visionaries deliver new and emerging capabilities ahead of their market competitors, providing buyers with early access to enhanced security and administration. For example, Visionaries may offer features such as AI integrations, workflow automation, advanced UEBA, bidirectional integrations with native and third-party security tools, and broader TDIR capabilities. While Visionaries can influence the direction of technological development in the market, they may not yet demonstrate a consistent track record of execution and often lack market share. Customers choose Visionaries for early access to innovative features.

Niche Players

Niche Players are primarily vendors that provide SIEM technology that is a good match for a specific SIEM use case or a subset of the SIEM market's functional requirements. Niche Players focus on a particular segment of the client base, such as midsize organizations, service providers or a specific region or industry, or may provide a limited set of SIEM capabilities. In addition, Niche Players may have a small installed base or be limited, according to Gartner's criteria, by other factors. These factors may include limited investments or capabilities, a geographically limited footprint or other inhibitors to providing a broad set of capabilities to organizations now and during a 12-month planning period.

Context

The SIEM market continues to react to customer demands, such as cost control, complexity reduction and better support for cloud environments. This Magic Quadrant emphasizes capabilities that support meeting these objectives, such as data management options, workflow augmentation powered by both AI and automation, integration with broader vendor-provided ecosystem solutions and support for cloud environments.

Readers should leverage this Magic Quadrant research as one of many resources to aid in their buying decision not as the single source of truth. Readers should not infer that a vendor in the Leaders quadrant is, by default, the best choice for their particular use case or environment. Assess vendors based on individual business and security needs not where they are in the quadrant.

This research assesses vendors based on their solutions as offered through 2024 up to 25 February 2025 to include the strength of their SIEM products and roadmaps. The SIEM market continuously evolves, meaning this research is a point-in-time assessment. As such, readers should leverage the companion Critical Capabilities for Security Information and Event Management as an initial evaluation, which may include off-cycle updates throughout the year as vendors make significant changes that warrant a Critical Capabilities scoring update.

Market Overview

Despite numerous competitive market solutions and continuing challenges around cost, the SIEM market continues to show growth and resolve. From 2023 to 2024, the SIEM market grew by 17% to $6.8 billion (see **Market Share Analysis: Security Services, Worldwide, 2024**). The SIEM market is not only growing, it’s evolving. The primary reason buyers select SIEM remains constant for performing TDIR operations, as well as compliance and reporting. The secondary factors for selecting a SIEM are where the evolutions in SIEM are happening. Buyers seek SIEM platforms that are simpler to operate, provide better data management options to control cost and better support cloud environments.

These secondary factors are sparking innovation among SIEM vendors, adding features such as workflow augmentation (AI), TDIR ecosystem solutions, improved data management options and improved cloud environmental support.

SIEM technologies are a staple for security operations, with a long-standing position as a technology that has reached the Plateau of Productivity (see Hype Cycle for Security Operations, 2025). However, Gartner has seen evidence that the SIEM market itself has been disrupted by external forces listed below, which are causing clients to rethink the role of an SIEM and how to select the best technology for them:

- With more diverse resources and requirements to integrate with APIs, building parsers has increased the dependence on partnerships and ease of onboarding.
- SIEM buyers have grown increasingly frustrated by SIEM cost bloat and seek better data management options.
- With the rising use of TDIR platforms, the need for seamless integration becomes more pronounced. The client is looking to decrease SIEM complexity and operational burdens to drive better security results.

As such, SIEM buyers often inquire about solutions that better support these disruptive forces. Cybersecurity leaders may prefer SIEM solutions that better support their chosen cloud environment over other SIEM features or solutions that offer more flexible data management options. They may also prioritize solutions that greatly reduce complexity, either through workflow augmentation or a highly converged ecosystem that extends beyond just the SIEM solution.

Cybersecurity leaders are shifting to evaluating bundled solutions from vendors like Microsoft, Palo Alto Networks and CrowdStrike. These vendors, with SIEM solutions, have made their SIEM offerings inclusive of their broader cloud solutions, with bundled licensing for the SIEM and other solutions, making integrations into other cloud features their competitive differentiator.

Other SIEM vendors have focused on providing better alternatives for buyers to manage large-scale data ingestion, which is often to blame for SIEM cost bloat. Vendors here give buyers the choice of what data goes to the SIEM for premium outcomes, and what other data might be better served with less premium options, such as long-term retention and search.

Complexity reduction has driven vendors to experiment with competing approaches. Some vendors claim complexity reduction is best served by combining the SIEM with other parts of the security stack, such as endpoint detection and response/XDR, threat intelligence and exposure assessment. Acquiring multiple solutions from one vendor arguably reduces the operational overhead costs, but can limit the flexibility of the SOC to only using that suite of tools. Other vendors claim complexity reduction does not require an ecosystem of solutions to work together, but is best achieved by strategic use of workflow augmentation technology, such as AI and automation. This approach again aims to reduce operational complexity and guides users to more predictable outcomes.

These market drivers have created shifts in the vendor landscape. This year, four new vendors were added and nine were dropped from the SIEM Magic Quadrant. The commercial requirements for inclusion this year grew in annual revenue, number of clients and global reach due to the first-time addition of some larger vendors.

These market drivers have also changed the consideration of what vision and execution should be for vendors aspiring to be Leaders in the market. A vendor's vision of what an SIEM should be matters more given the evolving state of SIEM, as does how well they can execute in getting market adoption for their new vision.

Among SIEM vendors, these were the capabilities most differentiated by prospective buyers:

- **Workflow augmentation:** SIEM solutions incorporate AI into their solutions to act as a force multiplier for the SOC, and as such AI techniques are used in the areas of log collection, detection, enrichment and workflow augmentation within the SIEM. The expectation is that the SIEM solutions offer reliable natural language querying, suggested remediation actions and advanced trend identification, allowing for data contextualization, specific questions and suggested automations in all these areas (see Prepare for SIEM Evolution).
  - During the evaluation process, we are seeing new features being released at a rapid rate of change. There are some clear areas where AI support is improving the onboarding process of sources, integrating APIs where they don't exist, and supporting complex queries across multiple external data sources.
  - However, this shift does not mean SOC teams will face less work or reduced complexity. In reality, as automation handles the simplest issues and reduces the viability of certain attack types, it also frees up the SOC to focus on more complex

threats (see **Predict 2025: There Will Never Be an Autonomous SOC**). Evaluate AI capabilities by comparing their impact against manual processes and tracking performance. Accuracy and transparency are critical as SOC teams must be able to operate effectively without AI in case of failure or loss of trust in the solution.

- **Data management options:** Data management has been a key factor for years; however, the bar has risen to include consideration for even more flexible data management options. Some vendors had solutions similar in value to telemetry pipeline management, while others offered flexible data stores and licensing options to help customers better manage SIEM cost bloat.

- **Cloud-native support:** Effectively monitoring cloud environments requires a flexible SIEM architecture and data ingestion capabilities that support distributed sources and larger volumes.

  - As cloud-native technologies expand into different domains, securing cloud-native environments becomes more complex and relevant, as such, organizations are demanding more enterprise-ready, cloud-native solutions that can cover specific security use cases.

Note 1: Cloud-Native Definition

Gartner defines “cloud-native” as something that is designed to leverage cloud characteristics. Those cloud characteristics are part of the original definition of cloud computing. It’s all about capabilities delivered as a service and that are scalable and elastic, metered by use, service-based, ubiquitous by means of internet technologies, and shared.

Note 2: Incident Response Activities

Incident response activities might include functions such as verbose event recording, chain of custody, automated mitigation actions, and reporting.

Note 3: Production Customers Definition

Production customers are defined as those that have licensed the SIEM and are monitoring production environments with the SIEM.

Note 4: Geographic Regions

Geographic regions are defined as North America, Latin America, Europe, Middle East, Asia, Japan, Africa.

⊕ Evaluation Criteria Definitions